AMENDMENTS TO THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for scanning data read from storage, comprising:

[[a)]] receiving a request for data saved in storage from a central processing unit;

[[b)]] scanning the requested data for malicious code; and

[[c)]] transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

2. (Currently Amended) The method as recited in claim 1, wherein the storage ~~is selected from the group consisting~~includes at least one of a hard drive, compact disc-read only memory (CD-ROM), and a floppy disk.

3. (Cancelled)

4. (Previously Presented) The method as recited in claim 1, wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

5. (Previously Presented) The method as recited in claim 1, wherein the storage subsystem controller is coupled to the storage.

6. (Previously Presented) The method as recited in claim 1, wherein the scanning module includes software.

7. (Previously Presented) The method as recited in claim 1, wherein the scanning module includes hardware.

8. (Cancelled)

9. (Cancelled)

10. (Original) The method as recited in claim 1, and further comprising executing an event based on results of the scanning.

11. (Original) The method as recited in claim 10, wherein the event includes an alert.

12. (Original) The method as recited in claim 10, and further comprising disabling the scanning module in response to the event.

13. (Original) The method as recited in claim 12, wherein data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

14. (Original) The method as recited in claim 1, wherein the scanning includes content scanning.

15. (Original) The method as recited in claim 1, wherein the scanning includes virus scanning.

16. (Original) The method as recited in claim 1, wherein the storage is accessible via a network.

17. (Currently Amended) A computer program product embodied on a tangible computer readable medium ~~for scanning data read from storage~~; comprising:

[[a)]] computer code for receiving a request for data saved in storage from a central processing unit;

[[b)]] computer code for scanning the requested data for malicious code; and

[[c)]] computer code for transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and the computer program product is operable such that data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

18. (Currently Amended) The computer program product as recited in claim 17, wherein the storage ~~is selected from the group consisting~~includes at least one of a hard drive, compact disc-read only memory (CD-ROM), and a floppy disk.

19. (Cancelled)

20. (Previously Presented) The computer program product as recited in claim 17, wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

21. (Previously Presented) The computer program product as recited in claim 17, wherein the storage subsystem controller is coupled to the storage.

22. (Previously Presented) The computer program product as recited in claim 17, wherein the scanning module includes software.

23. (Previously Presented) The computer program product as recited in claim 17, wherein the scanning module includes hardware.

24. (Cancelled)

25. (Cancelled)

26. (Currently Amended) The computer program product as recited in claim [[19]]17, and further comprising computer code for executing an event based on results of the scanning.

27. (Original) The computer program product as recited in claim 26, wherein the event includes an alert.

28. (Original) The computer program product as recited in claim 26, and further comprising computer code for disabling the scanning module in response to the event.

29. (Original) The computer program product as recited in claim 28, wherein data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

30. (Original) The computer program product as recited in claim 17, wherein the scanning includes content scanning.

31. (Original) The computer program product as recited in claim 17, wherein the scanning includes virus scanning.

32. (Original) The computer program product as recited in claim 17, wherein the storage is accessible via a network.

33. (Currently Amended) A method for scanning data written to storage, comprising:

[[a)]] receiving a request for data to be written in storage, the request being received from a central processing unit;

[[b)]] scanning the data for malicious code; and

[[c)]] writing the data to the storage if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module.

34. (Currently Amended) A computer program product embodied on a tangible computer readable medium ~~for scanning data written to storage~~, comprising:

[[a)]] computer code for receiving a request for data to be written in storage, the request being received from a central processing unit;

[[b)]] computer code for scanning the data for malicious code; and

[[c)]] computer code for writing the data to the storage if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and the computer program product is operable such that data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module.

35. (Currently Amended) A system ~~for scanning data read from storage~~, comprising:

[[a)]] storage for saving data therein;

[[b)]] a storage subsystem controller coupled to the storage for controlling access to the data saved therein;

[[c)]] a central processing unit coupled to the storage subsystem controller for issuing read requests for reading the data saved therein for processing purposes, and write requests for writing data to the storage;

[[d)]] a scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests; and

[[e)]] an event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning;

[[f)]] wherein the central processing unit is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning;

[[g)]] wherein a user is allowed to disable the scanning module, and the system is operable such that data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module.

36. (Original) The system as recited in claim 35, wherein the scanning module is coupled to the storage subsystem controller via a bus.

37. (Original) The system as recited in claim 35, wherein the scanning module is directly coupled to the storage subsystem controller.

38. (Previously Presented) The system as recited in claim 35, wherein the scanning module is coupled to the storage subsystem controller via a storage driver, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

39. (Currently Amended) A system ~~for scanning data read from storage~~, comprising:

[[a)]] means for saving data therein;

[[b)]] means for controlling access to the data saved therein;

[[c)]] means for issuing read requests for reading the data saved therein for processing purposes and write requests for writing data to the storage;

[[d)]] means for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests; and

[[e)]] means for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning;

[[f)]] wherein the central processing unit is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning;

[[g)]] wherein a user is allowed to disable the scanning module, and the system is operable such that data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module.

40. (Previously Presented) The method as recited in claim 1, wherein the user includes a remote administrator.

41. (Previously Presented) The method as recited in claim 1, wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage.

42. (Previously Presented) The method as recited in claim 41, wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled.

43. (Previously Presented) The method as recited in claim 42, wherein the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central processing unit.